Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney's Docket No. 10637-005002	Application No. 10/642,390
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Tomas Sander et al.	
(37 CFR §1.98(b))		Filing Date August 15, 2003	Group Art Unit ~~2131~~ 3621

U.S. Patent Documents

Examiner Initial	Desig. ID	Patent Number	Issue Date	Patentee	Class	Subclass	Filing Date If Appropriate
/P.L./	AA	4,759,063	07/19/88	Chaum			
	AB	4,995,082	02/19/91	Schnorr			
	AC	5,521,980	05/28/96	Brands			
	AD	5,604,805	02/18/97	Brands			
	AE	5,682,430	10/28/97	Kilian et al.			
	AF	5,708,780	01/13/98	Levergood et al.			
	AG	5,715,314	02/03/98	Payne et al.			
	AH	5,717,757	02/10/98	Micali			
	AI	5,724,424	03/03/98	Gifford			
	AJ	5,832,089	11/03/98	Kravitz et al.			
	AK	6,446,052	09/03/02	Juels			

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	AL	Baric et al., "Collision-Free Accumulators and Fail-Stop Signature Schemes Without Trees," Lecture Notes in Computer Science, 1997, 1233:480-494
	AM	Bayer et al., "Improving the Efficiency and Reliability of Digital Time-Stamping," Sequences II – Methods in Communication, Security, and Computer Science, 1992, pp. 329-334
	AN	Bellare et al,. "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," 1st ACM Conference on Computer and Communications Security, 1993, pp. 62-73
	AO	Bellare et al., "On Defining Proofs of Knowledge," Lecture Notes in Computer Science, 1992, 740:390-420
	AP	Bellare et al., "Round-Optimal Zero-Knowledge Arguments Based on Any One-Way Function," Advances in Cryptology: Proceedings of EUROCRYPT, 1997, pp. 280-305
	AQ	Bellare et al., "Translucent Cryptography – An Alternative to Key Escrow, and Its Implementation via Fractional Oblivious Transfer," J. Cryptology, 1999, 12:117-139
	AR	Benaloh et al., "Efficient Broadcast Time-Stamping," Technical Report 1, Clarkson University Department of Mathematics and Computer Sciences, 1992, Extended Abstract, 2 pgs.

Examiner Signature	Date Considered
/Peter Ludwig/	03/28/2007

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney's Docket No. 10637-005002	Application No. 10/642,390
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Tomas Sander et al.	
(37 CFR §1.98(b))		Filing Date August 15, 2003	Group Art Unit 2131

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	AS	Benaloh et al., "One-Way Accumulators: A Decentralized Alternative to Digital Signatures," Lecture Notes in Computer Science, 1994, pp. 274-285
	AT	Boneh et al., "Efficient Generation of Shared RSA Keys," Lecture Notes in Computer Science, 1997, 1233:425-439
	AU	Brands, "An Efficient Off-line Electronic Cash System Based on the Representation Problem," Centrum voor Wiskunde en Informatica Report, 1993, pp. 1-77
	AV	Brands, "Untraceable Off-line Cash in Wallet with Observers," Lecture Notes in Computer Science, 1993, 773:302-317
	AW	Brassard et al., "Non-Transitive Transfer of Confidence: A Perfect Zero-Knowledge Interactive Protocol for SAT and Beyond," IEEE, 1986, pp. 188-195
	AX	Brassard et al., "Minimum Disclosure Proofs of Knowledge," Journal of Computer and System Sciences, 1988, 37:156-189
	AY	Brickell et al., "Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change," Proceedings of the Sixth Annual ACM-SIAM Symposium on Discrete Algorithms,, 1995, pp. 457-466
	AZ	Camenisch et al., "An Efficient Fair Payment System," 3rd ACM Conference on Computer and Communications Security, 1996, New Delhi, India, pp. 88-94
	AAA	Camenisch et al., "Digital Payment Systems with Passive Anonymity-Revoking Trustees," Lecture Notes in Computer Science, 1996, 1146:33-43
	ABB	Camenisch et al., "A Group Signature Scheme with Improved Efficiency," Lecture Notes in Computer Science, 1998, 1514:160-174
	ACC	Camenisch et al., "Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes," Lecture Notes in Computer Science, 1999, 1592:107-122
	ADD	Carter et al., "Universal Classes of Hash Functions," Conference Record of the Ninth Annual ACM Symposium on Theory of Computing, May 2-4, 1977, Boulder, Colorado, pp. 106-112
	AEE	Chaum et al., "Untraceable Electronic Cash," Lecture Notes in Computer Science, 1988, pp. 319-327
	AFF	Chaum et al., "Transferred Cash Grows in Size," Lecture Notes in Computer Science, 1992, 658:390-407
	AGG	Chaum, "Blind Signatures for Untraceable Payments," Advances in Cryptology: Proceedings of Crypto - 82, 1983, pp. 199-203
	AHH	Chaum et al., "Electronic Money: Threat to Law Enforcement, Privacy, Freedom, or All Three?" Sixth Conference on Computers, Freedom and Privacy, 1996, pp. 68-73
	AII	Cohen et al., "A Robust and Verifiable Cryptographically Secure Election Scheme," IEEE, 1985, pp. 372-382
	AJJ	"Core Principles for Effective Banking Supervision," Basle Committee on Banking Supervision, Publication of the Bank for International Settlements, Basle, September 1997, pp. 1-46
	AKK	Cramer et al., "Signature Schemes Based on the Strong RSA Assumption," – Modification of an extended abstract in Proc. 6th ACM Conference on Computer and Communications Security, 1999, pp. 1-19
	ALL	Damgard, "Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals," Lecture Notes in Computer Science, 1990, pp. 328-335

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney's Docket No. 10637-005002	Application No. 10/642,390
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Tomas Sander et al.	
(37 CFR §1.98(b))		Filing Date August 15, 2003	Group Art Unit 2131

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	AMM	D'Amiano et al., "Methodology for Digital Money based on General Cryptographic Tools," Lecture Notes in Computer Science, 1995, 950:156-170
	ANN	Davida et al., "Anonymity Control in E-Cash Systems" Lecture Notes in Computer Science, 1997, 1318:1-16
	AOO	De Santis et al., "How to Share a Function Securely," Proc. 26th Annual ACM Symposium of the Theory of Computing, May 23-25, 1994, Montreal, Quebec, Canada, pp. 522-533
	APP	Dwork et al., "Digital Signets: Self-Enforcing Protection of Digital Information," Proc. 28th Annual ACM Symposium on the Theory of Computing, 1996, New York, pp. 489-498
	AQQ	"Electronic Money – Consumer Protection, Law Enforcement, Supervisory and Cross Border Issues," Report of the Working Party on Electronic Money, Publication of the Bank for International Settlements, Basle, April 1997
	ARR	"FATF-VII Report on Money Laundering Typologies," FinCEN Advisory, 1996, 1(4):1-14
	ASS	"FATF-IX Report on Money Laundering Typologies," Financial Crimes Enforcement Network Publications, February 1998
	ATT	Fiat et al., "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," Lecture Notes in Computer Science, 1986, 263:186-194
	AUU	Frankel et al., ""Indirect Discourse Proofs": Achieving Efficient Fair Off-Line E-cash," Lecture Notes in Computer Science, 1996, 1163:286-300
	AVV	Frankel et al., "Robust Efficient Distributed RSA-Key Generation," Proc. 39th Annual ACM Symposium on Theory of Computing, 1998, pp. 663-672
	AWW	Franklin et al., "Secure and Efficient Off-Line Digital Money," Lecture Notes in Computer Science, 1993, 700:265-276
	AXX	Fujisaki et al., "Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations," Advances in Cryptology – CRYPTO '97, 1997, pp. 16-30
	AYY	Fujisaki et al., "Practical Escrow Cash Systems," Lecture Notes in Computer Science, 1997, 1189:33-48
	AZZ	Gennaro et al., "Secure Hash-and-Sign Signatures Without the Random Oracle," Advances in Cryptology – EUROCRYPT '99, 1999, 1592:123-139
	AAAA	Goldreich et al., "How to Prove All NP Statements in Zero-Knowledge and a Methodology of Cryptographic Protocol Design," Lecture Notes in Computer Science, 1987, 263:171-185
	ABBB	Goldreich et al., "How to Ply Any Mental Game or A Completeness Theorem for Protocols with Honest Majority," Proc. 19th Annual ACM Symposium on Theory of Computing, May 1987, New York, pp. 218-229
	ACCC	Goldreich et al., "Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems," J. of the ACM, 1991, 38:691-729
	ADDD	Goldwasser et al., "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM J. Comput., 1988, 17(2):281-308
	AEEE	Goldwasser et al., "The Knowledge Complexity of Interactive Proof Systems," SIAM J. Comput., 1989, 18:186-208
	AFFF	Haber et al., "How To Time-Stamp a Digital Document," J. Cryptology, 1991, 3:99-111
	AGGG	Jakobsson et al., "Revokable and Versatile Electronic Money," 3rd ACM Conference on Computer and Communications Security, March 1996, New Delhi, India, pp. 76-87

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney's Docket No. 10637-005002	Application No. 10/642,390
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Tomas Sander et al.	
		Filing Date August 15, 2003	Group Art Unit 2131

(37 CFR 1.98(b))

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	AHHH	Jakobsson et al., "Mix-Based Electronic Payments," Fifth Annual Workshop on Selected Areas in Cryptography, 1998, pp. 157-173
	AIII	Jakobsson et al., "Improved Magic Ink Signatures Using Hints," Lecture Notes in Computer Science, 1999, 1648:253-267
	AJJJ	Juels et al., "Security of Blind Digital Signatures," CRYPTO: Proceedings of Crypto, 1997, pp. 150-164
	AKKK	MacKenzie et al., "Anonymous Investing: Hiding the Identities of Stockholders," Financial Cryptography, 1999, pp. 212-229
	ALLL	Merkle, "Protocols for Public Key Cryptosystems," IEEE, 1980, pp. 122-134
	AMMM	Molander et al., Cyberpayments and Money Laundering: Problems and Promise, RAND, 1998, http://www.rand.org/publications/MR/MR965/MR965.pdf/.
	ANNN	M'Raihi, "Cost-Effective Payment Schemes with Privacy Regulation," Lecture Notes in Computer Science, 1996, 1163:266-275
	AOOO	Naor et al., "Perfect Zero-Knowledge Arguments for *NP* Using Any One-Way Permutation," J. Cryptology, 1998, 11:87-108
	APPP	Nyberg, "Fast Accumulated Hashing," Lecture Notes in Computer Science, 1996, 1039:83-87
	AQQQ	Okamoto et al., "Disposable Zero-Knowledge Authentications and Their Application to Untraceable Electronic Cash," Advances in Cryptology: CRYPTO '89, 1990, pp. 481-496
	ARRR	Okamoto et al., "Universal Electronic Cash," Lecture Notes in Computer Science, 1992, 576:324-337
	ASSS	Petersen et al., "Efficient Scalable Fair Cash with Off-line Extortion Prevention," Lecture Notes in Computer Science, 1997, 1334:463-477
	ATTT	Pfitzmann et al., "How to Break and Repair a "Provably Secure" Untraceable Payment System," Lecture Notes in Computer Science, 1992, 576:338-350
	AUUU	Pointcheval et al., "Security Proofs for Signature Schemes," Lecture Notes in Computer Science, 1996, 1070:387-398
	AVVV	"Private Banking: Raul Salinas, Citibank, and Alleged Money Laundering," General Accounting Office (GAO) Report to the Ranking Minority Member, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, December 1998
	AWWW	"Risk Management for Electronic Banking and Electronic Money Activities," Basle Committee on Banking Supervision, Publication of the Bank for International Settlements, Basle, March 1998
	AXXX	Sander, "Efficient Accumulators Without Trapdoor," Proc. Of ICICS '99, 2nd International Conference on Information and Communication Security, 1999, pp. 252-262
	AYYY	Schnorr, "Efficient Signature Generation by Smart Cards," J. Cryptology, 1991, 4:161-174
	AZZZ	"Security of Electronic Money," Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries, Basle, August 1996
	AAAAA	Shamir, "On the Generation of Cryptographically Strong Pseudo-Random Sequences," Lecture Notes in Computer Science, 1981, 115:544-550
	ABBBB	Simon, "Anonymous Communication and Anonymous Cash," Lecture Notes in Computer Science, 1996, 1109:61-73

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney's Docket No. 10637-005002	Application No. 10/642,390
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR 1.98(b))		Applicant Tomas Sander et al.	
		Filing Date August 15, 2003	Group Art Unit 2131

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	ACCCC	Stadler et al., "Fair Blind Signatures," Lecture Notes in Computer Science, 1995, pp. 209-219
	ADDDD	Syverson et al., "Unlinkable Serial Transactions," Lecture Notes in Computer Science, 1997, 1318:39-55
	AEEEE	Tischler, "The Colombian Black Market Peso Exchange," Testimony before the Senate Caucus on International Narcotics Control, June 1999
	AFFFF	von Solms et al., "On Blind Signatures and Perfect Crimes," Computers & Security, 1992, 11:581-583
	AGGGG	Yao, "How to Generate and Exchange Secrets," IEEE, 1986, pp. 162-167

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute Disclosure Form (PTO-1449)